



Baker & Hostetler LLP

1170 Peachtree Street
Suite 2400
Atlanta, GA 30309-7676

T 404.459.0050
F 404.459.5734
www.bakerlaw.com

John P. Hutchins
direct dial: 404.946.9812
jhutchins@bakerlaw.com

May 8, 2024

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

Anthony G. Brown
Attorney General
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Incident Notification

Dear Attorney General Brown:

We are writing on behalf of our client, The Dufresne Spencer Group, LLC (the “Dufresne Spencer Group”), to notify your office of a cybersecurity incident that involved Maryland residents’ information.

The Dufresne Spencer Group detected unusual network activity, which was determined to be the result of a cybersecurity involving an unauthorized party. Upon discovering the incident, the Dufresne Spencer Group took immediate steps to secure its systems, launched an investigation with the assistance of cybersecurity experts and notified law enforcement.

The investigation determined that an unauthorized party accessed and/or acquired certain files stored on its servers. A thorough review of those files was conducted using both technology and a manual review, so that it could be determined who and what may have been affected by this incident. To meet these goals, legal counsel engaged outside analytics firms to identify individuals whose information may have been involved, the nature of any such information, and to collect address information. The Dufresne Spencer Group determined on January 15, 2024, following the conclusion of each data review that customer information was likely impacted, including the name, date of birth, Social Security number, financial account number, digital signature, and/or driver’s license number of 51 Maryland residents.

May 8, 2024

Page 2

Notifications were undertaken after the time-consuming process of collection and verification of up-to-date contact details and assembling appropriate resources to address any follow up inquiries.

On May 8, 2024, the Dufresne Spencer Group will be mailing notification letters to Maryland residents via U.S. First-Class mail in accordance with Md. Code Ann., Com. Law § 14-3504.¹ A copy of the notification is enclosed. The Dufresne Spencer Group is offering one year of complimentary credit monitoring, fraud consultation, and identity theft restoration services through Equifax to the Maryland residents whose Social Security number or driver's license number was involved in the incident. In addition, a dedicated toll-free call center has been established that individuals can call to obtain more information regarding the incident.

To reduce the risk of a similar incident from occurring in the future, the Dufresne Spencer Group has and will continue to take steps to enhance the security of its computer systems and the data it maintains.

Please do not hesitate to contact me if you have any questions regarding this matter.

John P. Hutchins

John P. Hutchins

Attachment

¹ This report does not waive the Dufresne Spencer Group's objection that Maryland lacks regulatory authority over it related to any claims that may arise from this incident.



Dufresne Spencer Group
4120 Air Trans Road
Memphis TN 38118

April 30, 2024

00695 ADFFIN G0145 L001 AUTO *000001



HOUSTON TX 77077

Dear [REDACTED]:

The Dufresne Spencer Group, LLC (the "Dufresne Spencer Group") addressed a data security incident that may have involved some of your information. This letter explains the incident, the measures we have taken, and some steps you may consider taking in response.

Upon identifying the data security incident, we immediately took steps to secure our systems and began an investigation with assistance from a cybersecurity firm. The investigation determined that an unauthorized party gained access to our information technology environment between May 15-June 5, 2023. During that time, the unauthorized party accessed and/or acquired files on our systems that contain personal information. We conducted a review of those files and determined on January 15, 2024 that some of your information, including: name, date of birth, driver's licence, banking information (i.e., account number, routing number), digital signature, has likely been impacted.

As a precaution, we are offering you a complimentary one-year membership to Equifax Credit Watch Gold credit monitoring and identity theft support. This product helps detect possible misuse of your personal information and provides you with identity protection support. Information about Equifax Credit Watch Gold and instructions on how to activate your complimentary one-year membership are included with this letter on the following page. You have until August 31, 2024 to activate your identity monitoring services.

We encourage you to remain vigilant by reviewing your financial account statements and credit reports for any unauthorized activity. If you see charges or activity you did not authorize, please contact the relevant financial institution or credit bureau reporting the activity immediately. For more information on additional steps you may consider taking, please see the pages that follow this letter.

We regret any inconvenience or concern this incident may cause. We have enhanced our existing security protocols and technical safeguards to help prevent issues like this in the future. We have established a dedicated call center to help answer frequently asked questions you may have about the incident. Please call 1-888-841-4262, Monday through Friday, between 9:00 a.m. and 9:00 p.m. Eastern with any questions you may have.

Sincerely,

Mike Linton, Chief Financial Officer

00695-ADFFIN-G0145-L001-AUTO-000001-000-1/2





Activation Code: 323910153738
Enrollment Deadline: August 31, 2024

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁴

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of **323910153738** then click “Submit” and follow these 4 steps:

1. **Register:**
Complete the form with your contact information and click “Continue”.
If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
 2. **Create Account:**
Enter your email address, create a password, and accept the terms of use.
 3. **Verify Identity:**
To enroll in your product, we will ask you to complete our identity verification process.
 4. **Checkout:**
Upon successful verification of your identity, you will see the Checkout Page. Click ‘Sign Me Up’ to finish enrolling.
- You’re done!**
The confirmation page shows your completed enrollment. Click “View My Product” to access the product features.

¹WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

²The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

³Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com

⁴The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877- IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two credit bureaus, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active-Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to do so.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.



The Dufresne Spencer Group can be reached at (901) 509-8860 and the address of its headquarters is 4120 Air Trans Rd, Memphis, TN 38118.

Additional information for residents of the following states:

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Place, 9th Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection> and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Rhode Island: This incident involves 7 individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

Additional Information for Residents of New Mexico:

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.